RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

LA CYBERSÉCURITÉ POUR LES TPE/PME EN 13 QUESTIONS

SOMMAIRE

Avant-propos 2

Questions :

N°1 – Connaissez-vous bien votre parc informatique et vos actifs métier ? 4

N°2 – Effectuez-vous des sauvegardes régulières ? 6

N°3 – Appliquez-vous régulièrement les mises à jour ? 9

N°4 – Utilisez-vous un antivirus ? 11

N°5 – Avez-vous implémenté une politique d'usage de mots de passe robustes ? 12

N°6 – Avez-vous activé un pare-feu ? En connaissez-vous les règles de filtrage ? 15

N°7 – Comment sécurisez-vous votre messagerie ? 17

N°8 – Comment séparez-vous vos usages informatiques ? 19

N°9 – Comment maîtrisez-vous le risque numérique lors des missions et des déplacements professionnels ? 21

N°10 – Comment vous informez-vous ? Comment sensibilisez-vous vos collaborateurs ? 24

N°11 – Avez-vous fait évaluer la couverture de votre police d'assurance au risque cyber ? 26

N°12 – Savez-vous comment réagir en cas de cyberattaque ? 27

N°13 – Envisagez-vous d'utiliser des solutions *cloud* ? 29

AVANT-PROPOS

En réduisant les coûts de certains investissements, en optimisant les processus et en rapprochant les entreprises de leurs clients, de leurs partenaires ou encore des services publics, la numérisation apporte d'incroyables opportunités aux TPE et aux PME. Il n'est désormais plus question de se passer des bénéfices formidables de ces nouveaux outils.

Mais cette transformation s'accompagne de risques réels qui ne cessent de s'intensifier, le nombre d'attaques informatiques augmentant de façon dramatique. Vol de données, demandes de rançon, atteinte à l'image ou sabotage sont autant de risques qui pèsent sur les organisations, avec des conséquences souvent graves, parfois irréversibles.

Cette réalité peut encore sembler abstraite, très technique, complexe et coûteuse pour les entreprises, notamment les plus petites, si bien qu'elles ne se préparent pas toujours suffisamment. Les conséquences sont pourtant très concrètes : si à la suite d'une attaque vos données disparaissent et votre informatique s'arrête, êtes-vous prêts à retourner au papier et au crayon ?

Sans compter que les structures de taille petite, moyenne et intermédiaire sont particulièrement à risque : en l'absence de dispositifs de protection, elles sont une cible de choix pour les acteurs malveillants qui optimisent leurs gains en attaquant les plus vulnérables. Et si les entreprises les mieux préparées peuvent se remettre d'une attaque informatique, d'autres en sont durablement affectées.

Heureusement, nous pouvons aussi regarder le sujet de façon plus positive. Voire, faire de la « cyber » une opportunité ! Car en se protégeant –et, par capillarité, en protégeant leurs partenaires– les entreprises assurent leur pérennité et renforcent la confiance qui les lie à leurs parties prenantes. La cybersécurité représente donc un enjeu collectif majeur. Plus largement, elle est une clé essentielle pour le développement économique durable de la nation.

Il y a une autre bonne nouvelle toutefois : l'application de quelques bonnes pratiques permet déjà de réduire très significativement le risque. En mettant en place quelques mesures simples mais essentielles, vous pourrez protéger votre entreprise contre de nombreuses cybermenaces, considérablement limiter les dégâts en cas d'attaque et faciliter le redémarrage de votre activité en cas d'incident avéré. Il n'y a pas de solution miracle ou de risque zéro mais chaque organisation peut faire beaucoup pour sa propre sécurité !

Complémentaire au guide d'hygiène informatique de l'ANSSI, ce guide présente, en treize questions, des mesures accessibles pour une protection globale de l'entreprise. À vous de vous en emparer pour protéger votre activité et vos emplois. Certaines recommandations relèvent des bonnes pratiques, d'autres requièrent un investissement plus important pour lequel votre structure pourra être accompagnée. Elles vous permettront d'accroître votre niveau de sécurisation et de sensibiliser vos équipes aux bons gestes à adopter.

En l'absence de préparation, lorsque l'incident survient, il est déjà trop tard. N'attendons pas que le pire arrive. Protégeons-nous !

Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

Thomas Courbe, directeur général des entreprises (DGE)

Avec le soutien de Cybermalveillance.gouv.fr, de France Num et de la Confédération des petites et moyennes entreprises (CPME).

QUESTION N°1

CONNAISSEZ-VOUS BIEN VOTRE PARC INFORMATIQUE ET VOS ACTIFS MÉTIER ?

PUBLIC : TOUS
DIFFICULTÉ : FACILE À MOYENNE

« Ai-je connaissance des systèmes d'informations, des applications et des données vitales pour mon entreprise au regard de mon activité ? » : cette question est la toute première à se poser pour renforcer le système d'information (SI) de son entreprise. **Pour bien se protéger, toute entreprise même unipersonnelle se doit d'inventorier ses matériels et ses logiciels ainsi que les données et les traitements qui constituent son patrimoine informationnel et contribuent à sa pérennité**. De cet inventaire découleront les mesures de protection adaptées.

Inventoriez tous les équipements et les services

Ordinateur (et ses périphériques), mobile multifonction, tablette, serveur local, serveur distant (hébergement du site Web, service de messagerie, services logiciels en ligne, etc.). **Il faut aussi inventorier tous les périphériques : box, commutateurs, clés 4G, imprimantes etc**. Cet inventaire permet de savoir quoi protéger et d'identifier dans une phase ultérieure, les biens critiques pour l'activité de l'entité.

Inventoriez les logiciels utilisés

Il faut connaître leur nature, leurs fonctions principales et leurs versions. Il faut également s'assurer d'être en possession de licences d'utilisation valides, qui sont indispensables aussi bien du point de vue des obligations légales, que pour la maintenance.

Inventoriez les données et les traitements de données

Quelles sont les données susceptibles d'affecter ou d'interrompre l'activité en cas de perte ou d'altération ? Quelles sont les données soumises à des obligations légales ? Y a-t-il un fichier client ? Où sont conservées les données, par exemple la comptabilité ? La même question se pose pour les traitements : quels sont les traitements dont l'altération affecterait ou interromprait particulièrement l'activité ? Les traitements et les données sont-ils manipulés en local ou dans un *cloud* public ?

Inventoriez tous les accès

Il s'agit ici de déterminer qui se connecte au système d'information et quelles sont les modalités de chaque accès : catégorie de l'accédant (administrateur, utilisateur, invité), moyen d'accès (connexion locale ou distante), etc. Cet inventaire permettra de vérifier qu'aucun accès indu n'est maintenu (ancien employé, ancien prestataire) et ainsi de limiter la surface d'exposition aux menaces.

Inventoriez les interconnexions avec l'extérieur

Quels sont les points de contact entre le système d'information de l'entreprise et Internet ? **Tout accès Internet, vers un prestataire ou un partenaire doit être recensé pour figurer ensuite dans l'inventaire, de même que les accès des employés au système d'information de l'entreprise** (ex : nomadisme). Des règles de filtrage et de surveillance adaptées pourront y être associées.

Ce bilan indispensable permet de faire le point sur les besoins et les capacités numériques de son entreprise ; il doit être mis à jour régulièrement, et au moins une fois par an. Il permet également d'aider au choix des solutions numériques adaptées à l'entreprise, d'identifier les éventuels points de sécurisation à envisager et, le cas échéant, de fournir un état des lieux détaillé qui aidera le prestataire sollicité pour cette tâche. Il sera aussi très utile pour les professionnels qui interviendront en réponse à un incident en cas de compromission réelle.

POUR EN SAVOIR PLUS :
www.ssi.gouv.fr/guide/cartographie-du-systeme-dinformation

QUESTION N°2

EFFECTUEZ-VOUS DES SAUVEGARDES RÉGULIÈRES ?

PUBLIC : TOUS
DIFFICULTÉ : FACILE À MOYENNE

Effectuer des sauvegardes régulières permet une restauration plus rapide des activités opérationnelles en cas d'incident, notamment en cas d'attaque par rançongiciel.

Identifiez les données à sauvegarder

Afin d'identifier les données, vous devez avoir inventorié préalablement tous vos matériels puis déterminer quelles données sont essentielles à la poursuite de votre activité. Il peut s'agir de « données métier » (fichiers client, savoir-faire de fabrication par exemple), mais peut-être également des données techniques. Ces dernières peuvent concerner la configuration des ordinateurs ou de tout ou partie de l'infrastructure de l'entreprise, notamment pour les outils de production industrielle. Enfin, **il est important de sauvegarder les sources d'installation, les licences et les fichiers de configuration des applications.**

Déterminez le rythme de vos sauvegardes

La fréquence des sauvegardes est à définir en lien avec le volume de données numériques produites sur un temps donné. Par exemple, une TPE/PME dans le secteur de l'artisanat pourra choisir une fréquence mensuelle de sauvegarde de ses factures et de son fichier client. En revanche, une TPE/PME de services pour qui les échanges dématérialisés constituent la valeur marchande, pourra choisir une fréquence accrue avec des sauvegardes hebdomadaires voire quotidiennes. Une sauvegarde différentielle peut être mise en place afin de retrouver différents points de sauvegarde : chaque jour ou chaque semaine pour les données métier, et chaque mois pour les données techniques.

Choisissez le ou les supports à privilégier pour votre sauvegarde

Pour plus de souplesse et de résilience, il convient de s'appuyer sur des sauvegardes en ligne mais également sur des sauvegardes déconnectées. Les sauvegardes en ligne, par exemple sur des disques réseaux (SAN/NAS) ou des services nuagiques (*cloud*) permettent une fluidité et une agilité des sauvegardes. En revanche, elles sont exposées aux attaques informatiques, telles que les rançongiciels. Parce que le système de sauvegarde est connecté au réseau, un cyberattaquant est susceptible de parvenir à accéder aux sauvegardes, de voler les informations qu'elles contiennent, voire de les chiffrer pour les rendre inexploitables par leur propriétaire. Il est donc nécessaire de compléter le dispositif de sauvegarde par des sauvegardes dites « hors ligne » ou déconnectées. Il peut s'agir d'un support physique comme un disque dur externe, à déconnecter impérativement du système d'information à l'issue de la sauvegarde. Ce type de support réduit le risque d'une compromission des données qu'il contient mais n'est pas à l'abri d'un vol, d'une destruction ou d'un dysfonctionnement. Certains services nuagiques spécialisés peuvent apporter les garanties de déconnexion recherchées. Mais ceux-ci doivent être explicitement souscrits auprès du fournisseur de service nuagique et leur efficacité doit être vérifiée. **Appliquez la règle simple « 3-2-1 » : 3 copies de sauvegarde, sur 2 supports différents dont 1 hors ligne.**

Quel que soit votre choix de supports, **les sauvegardes doivent faire l'objet de tests réguliers de restauration pour garantir qu'elles seront exploitables le moment venu** (et particulièrement après un incident de sécurité majeur de type attaque par rançongiciel).

Évaluez la pertinence du chiffrement des données

Le chiffrement des données avant leur sauvegarde est une pratique recommandée. Elle concerne aussi le stockage dans un service nuagique : en cas d'accès illégitime au service nuagique, les données restent protégées à la condition que les clés de chiffrement soient correctement gérées. Le choix de l'opérateur nuagique, les modalités de stockage des données et les conditions d'accès et d'authentification seront autant de points de vigilance à vérifier.

Il est important de définir qui détient les clés de chiffrement des sauvegardes et de préciser la manière dont celles-ci sont elles-mêmes sauvegardées.

Respectez le cadre juridique

Les données dites « personnelles », qu'elles soient relatives aux employés ou à la clientèle, nécessitent des mesures de protection renforcées pour ▶

garantir leur intégrité, leur confidentialité, leur disponibilité et leur résilience en application du règlement général sur la protection des données (RGPD). **Les dispositifs juridiques de protection et de conservation des données s'appliquent quels que soient les objectifs du stockage (traitement ou sauvegarde)**. Qu'il s'agisse des obligations fiscales ou de protection des données personnelles, appliquez les mêmes mesures à vos sauvegardes qu'à votre système d'information.

POUR EN SAVOIR PLUS :

- www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes
- www.ssi.gouv.fr/administration/reglementation/rgpd-renforcer-la-securite-des-donnees-a-caractere-personnel
- www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident

QUESTION N°3

APPLIQUEZ-VOUS RÉGULIÈREMENT LES MISES À JOUR ?

PUBLIC : TOUS
DIFFICULTÉ : FACILE À MOYENNE

Au-delà des attaques s'appuyant sur la négligence des utilisateurs et sur l'ingénierie sociale, la majorité des attaquants exploitent des vulnérabilités publiques et documentées pour prendre pied sur les systèmes d'information. Ces vulnérabilités concernent principalement des services exposés sur Internet (par exemple un pare-feu, un serveur de messagerie, un service d'accès nomade, etc.). Qui plus est, les délais entre la publication d'une vulnérabilité et son exploitation par les cyberattaquants ont tendance à diminuer. Certaines campagnes d'attaques massives et récentes ont industrialisé l'exploitation de vulnérabilités seulement quelques jours après leurs révélations sur Internet.

Il est indispensable d'effectuer, dès que possible, les mises à jour des systèmes d'exploitation et de tout logiciel dès la mise à disposition des correctifs de sécurité par leurs éditeurs.

Utilisez des solutions matérielles et logicielles maintenues

Par habitude, par négligence ou par souci d'économies, il peut sembler tentant de conserver un matériel ou un logiciel au-delà de la période durant laquelle son fabricant ou son éditeur garantit son maintien en conditions de sécurité. Tout matériel ou logiciel qui ne peut plus être mis à jour doit être désinstallé et remplacé.

Activez la mise à jour automatique des logiciels et des matériels

Les mises à jour du système d'exploitation et de tous les logiciels utilisés doivent être effectuées dès que possible, à chaque mise à disposition d'un correctif par leurs éditeurs. Cela est d'autant plus important pour tous les matériels ▶

et les logiciels accessibles depuis Internet.

Il est recommandé d'activer les fonctions de mise à jour automatique proposées par les éditeurs.

Outre ces mises à jour régulières, des mises à jour hors calendrier peuvent survenir en cas de détection d'une vulnérabilité dont la criticité ne permet pas d'attendre plusieurs semaines pour le déploiement d'un correctif. Ces mises à jour doivent aussi être appliquées dès que possible.

Si vous recourez à un sous-traitant

Assurez-vous qu'il effectue bien la mise à jour des systèmes numériques utilisés dans votre entreprise. Si nécessaire, exigez cette pratique dans vos contrats de sous-traitance.

POUR EN SAVOIR PLUS :

- www.ssi.gouv.fr/guide/guide-dhygiene-informatique
- www.ssi.gouv.fr/guide/externalisation-et-securite-des-systemes-dinformation-un-guide-pour-maitriser-les-risques
- www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mises-a-jour

QUESTION N°4

UTILISEZ-VOUS UN ANTIVIRUS ?

PUBLIC : TOUS
DIFFICULTÉ : FACILE

Les antivirus sont très utiles à la protection des moyens informatiques : ils constituent une première ligne de défense contre les attaquants. **Un antivirus doit être déployé sur la majorité des équipements informatiques**, en priorité ceux connectés à Internet (postes de travail, serveurs de fichier, etc.). Un antivirus protège des menaces connues qui évoluent très rapidement : des centaines de milliers de codes malveillants apparaissent chaque jour.

Il faut, pour cette raison, tenir à jour le logiciel en lui-même et sa base de données de signatures. Cette base de données est l'élément qui permet l'identification de programmes et de fichiers malveillants : sans sa mise à jour fréquente, la protection offerte par l'antivirus s'en trouve très rapidement plus restreinte.

Les antivirus commerciaux proposent **une mise à jour automatique**, et un scan automatique des espaces de stockage : il est indispensable de procéder à l'activation de ces mécanismes dans les paramètres.

Par ailleurs, lors de l'achat d'un antivirus, il peut être intéressant, en fonction de vos usages, de souscrire aux fonctionnalités complémentaires proposées par de nombreux éditeurs logiciels tels qu'un pare-feu, un filtrage Web, des outils anti-hameçonnage et de renforcement de la sécurité des transactions bancaires.

QUESTION N°5

AVEZ-VOUS IMPLÉMENTÉ UNE POLITIQUE D'USAGE DE MOTS DE PASSE ROBUSTES ?

PUBLIC : TOUS
DIFFICULTÉ : FACILE À MOYENNE

Pourquoi choisir des mots de passe robustes ?

De nombreuses attaques sur Internet sont facilitées par l'utilisation de mots de passe trop simples ou réutilisés d'un service à l'autre. Les attaques contre des mots de passe peuvent être de différentes natures : attaques par force brute (l'attaquant tente le plus grand nombre de combinaisons possibles) ou par dictionnaires (l'attaquant tente les mots de passe les plus courants, qu'il s'agisse de noms communs ou de combinaisons simplistes comme « azerty »). Les attaques peuvent aussi être de type « ingénierie sociale » : l'attaquant teste alors des informations personnelles telles que les prénoms de vos proches ou les surnoms de vos animaux de compagnie après les avoir récupérés sur les réseaux sociaux. Enfin, ces attaques peuvent être effectuées à partir d'éléments déjà disponibles en ligne, parfois à votre insu, tels qu'une base de données mal sécurisée d'un fournisseur où figureraient vos identifiants pour un service donné.

Il faut ajouter qu'une attaque contre les mots de passe peut ne pas avoir comme finalité de se limiter au service impacté, mais permettre une propagation de l'attaque au sein de l'entreprise ou à ses partenaires. Par exemple, votre courriel pourrait être utilisé par l'attaquant pour envoyer des courriels malveillants vers vos contacts professionnels afin de les inciter à faire des actions dangereuses à leur insu (comme cliquer sur un lien vers un site Internet compromis). Cette technique d'attaque porte le nom de hameçonnage (ou *phishing* en anglais).

Qu'est-ce qu'un mot de passe robuste ?

- **L'ANSSI recommande que la longueur d'un mot de passe soit corrélée avec la criticité du service auquel il donne accès**, avec un minimum de **9 caractères pour les services peu critiques** (dont la compromission ne donnerait accès à aucune information personnelle, financière et n'impacterait pas le fonctionnement de l'entreprise) et un minimum de **15 caractères pour les services critiques**.
- **Un mot de passe robuste comporte des capitales et des minuscules, des chiffres et des caractères spéciaux**.
- Ces mots de passe ne doivent comporter aucun élément personnel (tel qu'une date de naissance ou un prénom).
- Il est possible d'avoir recours à une phrase de passe (*passphrase* en anglais). Les phrases de passe consistent à choisir aléatoirement un certain nombre de mots parmi un corpus déterminé (comme le dictionnaire de la langue française). Les *passphrases* sont souvent bien plus longues que les mots de passe « classiques », mais sont aussi pour certains utilisateurs plus simples à mémoriser.

Qu'est-ce qu'une bonne politique de mots de passe ?

- **Il faut des mots de passe différents pour chaque service nécessitant une authentification**. Il convient en particulier de ne jamais utiliser un même mot de passe pour sa messagerie personnelle et sa messagerie professionnelle.
- Un coffre-fort de mots de passe peut vous aider à générer des mots de passe robustes et ne pas avoir à les mémoriser. Il permet de sauvegarder l'ensemble des mots de passe dans un fichier chiffré, accessible uniquement par un seul et unique mot de passe. Il est préférable d'utiliser un coffre-fort certifié par l'ANSSI.
- Le succès d'une bonne politique de choix des mots de passe nécessite une sensibilisation des utilisateurs aux risques liés à la sélection d'un mot de passe qui serait trop facile à deviner.
  Il faut activer une authentification multifacteurs quand elle est proposée par le fournisseur de service (mail, banque, etc.).
  De nombreux services permettent désormais de renforcer le mot de passe par une authentification secondaire : en plus du mot de passe, la saisie d'un second élément est nécessaire. Il est recommandé d'activer ce paramètre dès qu'il vous est proposé.

Faites-le choix d'une authenfication multifacteurs

- **Les mécanismes d'authentification multifacteurs offrent un niveau de sécurité supplémentaire qu'un simple mot de passe**. Désormais largement répandues, ces solutions s'appuient le plus souvent sur deux facteurs (on parle de « 2FA ») : un mot de passe mais aussi une confirmation par un code transmis via un mode de connexion tiers.
- **Simple d'utilisation, ces solutions sont proposées par de nombreux offreurs de services en ligne sur Internet (par exemple, pour les messageries électroniques, les services bancaires ou les accès aux services nuagiques ou *cloud*)**.

POUR LES PME

Il convient idéalement d'implémenter une authentification multifacteurs par jeton physique (carte à puce, token USB, etc.) pour simplifier l'accès aux terminaux de l'entreprise.

Pour les PME qui disposent de nombreuses solutions logicielles centralisées (messagerie, services Web internes, etc.), l'activation d'un service d'authentification unifié (type *single sign on*) permet de renforcer les mécanismes d'authentification et de simplifier l'expérience utilisateur.

Pour encadrer et vérifier l'application de ces règles, une PME pourra recourir à des mesures parmi lesquelles :

- le blocage des comptes à l'issue de plusieurs échecs de connexion, ce blocage pouvant être temporaire ou permanent ;
- la désactivation des options de connexion anonyme (comptes « invité ») ;
- la mise en place d'une politique robuste des mots de passe sur les serveurs d'authentification.

POUR EN SAVOIR PLUS :

- www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe
- www.ssi.gouv.fr/guide/mot-de-passe

QUESTION N°6

AVEZ-VOUS ACTIVÉ UN PARE-FEU ? EN CONNAISSEZ-VOUS LES RÈGLES DE FILTRAGE ?

PUBLIC : TOUS
DIFFICULTÉ : FACILE À EXPERT

Pourquoi activer le pare-feu local ?

Ce logiciel, installé sur l'ordinateur de l'utilisateur, protège principalement contre des attaques provenant d'Internet. Pour les entreprises disposant d'un système d'information d'entreprise, il permet également de ralentir ou de limiter l'action d'un acteur malveillant souhaitant prendre le contrôle d'un des postes de travail. Les attaquants tentent souvent d'étendre leur intrusion aux autres postes de travail et aux serveurs pour prendre entièrement le contrôle du système d'information et, *in fine*, accéder aux documents des utilisateurs. L'activation du pare-feu et une configuration adaptée rendent plus difficiles ces déplacements latéraux.

Comment procéder ?

POUR LES TPE

Sans connaissance informatique particulière, l'activation d'un pare-feu préinstallé sur le poste de travail et son paramétrage par défaut (qui bloque toute connexion entrante), constituent un premier niveau de protection. Un pare-feu local est une fonction intégrée à la plupart des systèmes d'exploitation grand public. Des pare-feux sont également commercialisés en complément de suites logicielles antivirales.

POUR LES PME

Un pare-feu local (qu'il soit intégré au système d'exploitation ou qu'il

soit une solution logicielle tierce), doit être installé sur tous les postes de travail. Il est recommandé d'assurer l'homogénéité des configurations et de la politique de filtrage des flux.

Une politique de filtrage minimale :

- bloque tous les flux non strictement nécessaires (en particulier les connexions entrantes depuis Internet) ;
- journalise les flux bloqués.

Par ailleurs, une PME doit déployer des pare-feux physiques en priorité pour protéger l'interconnexion du SI à Internet, voire, pour les entités les plus matures en matière de sécurité ou disposant d'une masse critique, pour segmenter le réseau interne en zones ayant des niveaux différents de sensibilité et d'exposition aux menaces (zone des postes de travail utilisateurs, zone des serveurs internes, zone des serveurs exposés sur Internet, zone des systèmes industriels et des outils de production, etc.).

S'agissant de l'interconnexion à Internet, elle se traduira idéalement par la mise en œuvre d'une zone « démilitarisée » (DMZ), constituée de pare-feux mais aussi de services de rebond, principalement pour la messagerie et la navigation Web.

Pour une configuration adaptée à vos usages, n'hésitez pas à recourir aux services d'un prestataire informatique labellisé ExpertCyber. Une mise en relation est proposée par le site Cybermalveillance.gouv.fr.

POUR EN SAVOIR PLUS :
Mise en œuvre de pare-feux physiques : www.ssi.gouv.fr/uploads/2018/01/guide_preconisations-pare-feux-zone-exposee-internet_anssi_pa_044_v1.pdf

QUESTION N°7

COMMENT SÉCURISEZ-VOUS VOTRE MESSAGERIE ?

PUBLIC : TOUS
DIFFICULTÉ : FACILE À MOYENNE *(TPE)* **/ MOYENNE À EXPERT** *(PME)*

POUR LES TPE

La messagerie est un autre vecteur principal d'infection du poste de travail, qu'il s'agisse de l'ouverture de pièces jointes contenant un code malveillant ou du clic malencontreux sur un lien redirigeant vers un site lui-même malveillant (*phishing* ou hameçonnage).

Quelques réflexes permettent de se prémunir des tentatives d'hameçonnage : l'expéditeur est-il connu ? Une information de sa part est-elle attendue ? Le lien proposé est-il cohérent avec le sujet évoqué ? En cas de doute, une vérification de l'authenticité du message par un autre canal (téléphone, SMS, etc.) auprès de l'émetteur est nécessaire.

Par ailleurs, la redirection de messages professionnels vers une messagerie personnelle est à proscrire car cela constitue un vecteur de fuite irrémédiable d'informations de l'entité.

Il est vivement recommandé de se doter, en complément d'un antivirus, d'un anti-spam et d'une solution anti-*phishing* pour augmenter les capacités de détection des tentatives d'hameçonnage.

Enfin, les offres nuagiques (*cloud*) de messageries électroniques doivent également être considérées par les entreprises. Celles-ci peuvent éviter aux entreprises la charge de la gestion des infrastructures de messageries. La plupart d'entre elles apportent par ailleurs les fonctions de sécurité requises (authentification multifacteurs, sauvegardes, anti-spam, etc.). Si un tel choix devait être fait, les entreprises doivent s'assurer que ses fonctions de sécurité sont bien présentes et configurées de manière à être actives.

POUR LES PME

Que l'entité héberge ou fasse héberger son système de messagerie, elle doit s'assurer :

- de disposer d'un système d'analyse antivirus en amont des boîtes aux lettres des utilisateurs pour prévenir la réception de fichiers infectés ;
- de l'activation du chiffrement TLS des échanges entre serveurs de messagerie (de l'entité ou publics) ainsi qu'entre les postes utilisateurs et les serveurs hébergeant les boîtes de messagerie électronique, en particulier pour les phases d'authentification.

Pour se prémunir d'escroqueries connues (par exemple, une demande de virement frauduleux émanant vraisemblablement d'un dirigeant), des mesures organisationnelles doivent être appliquées strictement.

Il est souhaitable de ne pas exposer directement les serveurs de messagerie électronique d'entreprise sur Internet. Dans ce cas, un serveur relais dédié à l'envoi et à la réception des messages doit être mis en place en coupure d'Internet.

POUR EN SAVOIR PLUS :

- www.ssi.gouv.fr/entreprise/precautions-elementaires/5-reflexes-a-avoir-lors-de-la-reception-dun-courriel
- www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing
- www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-tls

QUESTION N°8

COMMENT SÉPAREZ-VOUS VOS USAGES INFORMATIQUES ?

PUBLIC : TOUS
DIFFICULTÉ : FACILE À MOYENNE

L'interconnexion des outils informatiques avec Internet présente un certain nombre de risques, parmi lesquels on peut citer :

- l'exfiltration de données depuis l'entreprise vers Internet, portant ainsi atteinte à leur confidentialité voire à la réputation de l'entreprise (en particulier si elles sont diffusées) ;
- l'intrusion depuis Internet pour porter atteinte à l'intégrité ou la disponibilité du SI et des outils de production de l'entreprise ;
- l'usurpation d'identité ;
- le détournement de finalité du SI de l'entreprise pour des usages frauduleux ou délictueux.

Comment diminuer l'exposition à ces menaces ?

Un premier principe d'hygiène repose sur la création de comptes utilisateurs dédiés à chaque employé et ne disposant pas de privilège d'administration. Cette mesure permet de réduire le risque d'installation de codes malveillants.

Seuls les comptes utilisateur doivent être utilisés pour la navigation sur Internet : en effet, de très nombreuses attaques sont causées par une navigation effectuée depuis un compte doté de privilèges élevés, ce qui facilite grandement la tâche d'un attaquant pour prendre le contrôle complet de l'ordinateur. Les comptes d'administration doivent être utilisés uniquement pour configurer les équipements ou installer des logiciels. **Les comptes et leurs privilèges doivent être tenus à jour : quand un collaborateur quitte l'entreprise, il convient de faire l'inventaire** de ses accès et de tous les révoquer, de telle sorte que lui-même ou **un tiers ne puisse plus en faire usage.**

Par ailleurs, l'idéal est d'utiliser un ordinateur uniquement dédié à sa pratique professionnelle, sans usage personnel et familial. Cependant en cas d'usages multiples sur une seule et même machine, il est alors recommandé de créer des comptes utilisateur pour chaque usage.

Ces cloisonnements d'usage sont faciles à implémenter même par un entrepreneur individuel, sur sa propre machine. Ils permettent de contrer l'exécution arbitraire d'un certain nombre de programmes malveillants. Depuis un mobile multifonctions ou une tablette, les tâches d'administration et de cloisonnement s'effectuent d'une autre manière : **il faut limiter les autorisations données à chaque application pour chacune de leurs utilisations et télécharger les applications uniquement depuis les magasins officiels d'applications.**

POUR LES PME

Les PME qui comportent un plus grand nombre de collaborateurs et un réseau informatique de plusieurs machines prendront également avantage à respecter les mesures suivantes, ou les faire appliquer par leur prestataire :

- Les connexions entre les postes des utilisateurs doivent être interdites par défaut (configuration du pare-feu local, voir la question n°6) : si un poste est infecté par un code malveillant, ce cloisonnement évite la propagation directe sur l'ensemble des autres postes.
- En matière d'administration du SI de l'entreprise, les postes et les comptes d'administration doivent être dédiés à cet usage.
- Si les ressources de l'entreprise s'y prêtent, les activités numériques de l'entreprise doivent être cloisonnées en différentes zones réseaux par des dispositifs de filtrage physiques ou virtualisés (zone des serveurs internes, zone des serveurs exposés sur Internet, zone des postes de travail utilisateurs, zone d'administration, zone système industriel, etc.). Il est recommandé de vous faire accompagner par des professionnels de l'informatique pour bénéficier de l'architecture sécurisée, adaptée à votre système d'information et à la nature de vos données.

POUR EN SAVOIR PLUS :
- www.ssi.gouv.fr/guide/definition-dune-architecture-de-passerelle-dinterconnexion-securisee
- www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-usages-pro-perso

QUESTION N°9

MAÎTRISEZ-VOUS LE RISQUE NUMÉRIQUE EN SITUATION DE NOMADISME ?

PUBLIC : TOUS
DIFFICULTÉ : FACILE *(TPE)* **/ FACILE À EXPERT** *(PME)*

L'emploi d'ordinateurs portables, de mobiles multifonctions (*smartphone*) ou de tablettes, facilite les déplacements professionnels ainsi que le transport et l'échange de données. La pratique du télétravail, du travail dans des lieux publics ou dans les transports en commun, présentent des enjeux de sécurité à prendre en compte, quelle que soit la taille de l'entreprise. Tout en facilitant la continuité d'activité, ces usages produisent en effet des risques spécifiques.

Quelles sont les principales menaces en nomadisme ?

- espionnage de vos informations sensibles (contrats, projets, etc.) ;
- piégeage de vos équipements (*keylogger*, etc.) ;
- vol de vos équipements, de vos informations personnelles et de connexions.

POUR LES TPE/PME

Sensibilisez vos collaborateurs aux bons réflexes

- sauvegardez régulièrement vos données pour être en mesure de les restaurer en cas de perte ou de vol des équipements ;
- équipez systématiquement vos équipements de filtres écran de confidentialité ;
- privilégiez, autant que possible, des modes d'authentification où vos mots de passe ne sont pas préenregistrés dans vos équipements ;

- procéder au chiffrement de vos données les plus sensibles ou de l'ensemble du disque dur. Dans tous les cas, ne pas oublier de configurer un mot de passe de déchiffrement d'urgence ;
- gardez vos appareils, supports et fichiers avec vous. Ne pas laisser vos équipements sans surveillance ;
- si jamais vous devez vous absenter, pensez systématiquement à verrouiller vos équipements, voire les éteindre. Configurez une durée de verrouillage automatique inférieure à 5 minutes ;
- informez votre entreprise en cas de perte ou de vol de votre matériel ;
- ne connectez pas vos équipements professionnels à des équipements qui ne sont pas de confiance :
  - refusez la connexion d'équipements appartenant à des tiers (*smartphone*, clé USB, etc.) sur vos postes ;
  - si vous devez recharger votre téléphone mobile, ne le connectez pas à un ordinateur tiers ou à une prise USB en libre-service mais utilisez votre propre chargeur électrique ;
  - ne connectez pas vos postes sur des portails captifs (commerces, hôtels, etc.), préférez un partage de connexion 4G/5G avec votre téléphone mobile ;
  - si vous avez besoin d'échanger des documents avec un tiers, préférez les échanges par mail ou utilisez une clé USB destinée uniquement à cet usage ;
- soyez vigilant quant à la confidentialité des échanges pendant vos appels téléphoniques et vos visioconférences.

POUR LES PME

Sensibilisez vos collaborateurs aux bons réflexes

- N'utilisez que du matériel (ordinateur, supports amovibles, téléphone) fourni par l'entreprise. Proscrire l'utilisation d'équipements personnels (imprimante, PC, etc.) et d'adresses mail personnelles pour des besoins professionnels.
- Dans le cas où vous devez accéder à distance aux systèmes d'information de l'entreprise, prévoyez l'installation d'un logiciel de connexion à distance de type VPN chiffré [1] (*virtual private network*) afin de protéger vos communications. Dans la mesure du possible, configurez le client VPN en mode *full-tunneling* [2].
- Ne pas exposer d'applications ou de données métier sensibles directement sur Internet (n'autoriser l'accès à celles-ci qu'au travers du VPN.
- Protégez l'accès au BIOS (*Basic Input Output System*) avec un mot de passe robuste et activez la fonction de *secure boot* sur vos postes.
- Sensibilisez vos collaborateurs aux risques du nomadisme (ex : évitez de travailler sur des documents sensibles dans le train, etc.).

Les déplacements professionnels à l'étranger font également l'objet de mesures spécifiques qui sont décrites dans le guide de l'ANSSI relatif à ce sujet (voir l'encart « Pour en savoir plus »).

POUR EN SAVOIR PLUS :
- www.ssi.gouv.fr/nomadisme-numerique
- www.ssi.gouv.fr/guide/partir-en-mission-avec-son-telephone-sa-tablette-ou-son-ordinateur-portable

1 Deux mécanismes de chiffrement sont principalement proposés pour les VPN : IPsec ou TLS.

2 L'ensemble des flux réseaux du poste transite via le tunnel VPN, une fois celui-ci établi.

QUESTION N°10

COMMENT VOUS INFORMEZ-VOUS ? COMMENT SENSIBILISEZ-VOUS VOS COLLABORATEURS ?

PUBLIC : TOUS
DIFFICULTÉ : FACILE À MOYENNE

POUR LES TPE : S'INFORMER

Sans avoir de compétences particulières en informatique ni beaucoup de temps à y consacrer, il est possible de prendre connaissance de recommandations concernant les bonnes pratiques, d'alertes sur les menaces en cours et d'informations sur les mises à jour logicielles disponibles en suivant les actualités publiées par le dispositif Cybermalveillance.gouv.fr. Ce suivi ne nécessite aucune compétence informatique particulière.

POUR LES PME : S'INFORMER ET SENSIBILISER

Pour aller plus loin, une veille technique relative aux campagnes d'attaques et aux vulnérabilités est également effectuée par le centre gouvernemental de veille, d'alertes et de réponse aux attaques informatiques : le CERT-FR. Elle conviendra plus particulièrement aux PME dotées d'un service informatique, mais aussi aux professionnels indépendants qui souhaitent élargir leurs connaissances.

Au-delà, pour les PME, il est recommandé de mettre en place les bases d'une culture de l'hygiène informatique par une information régulière du personnel aux bonnes pratiques de sécurité et aux principales menaces qui peuvent affecter la vie de l'entreprise. Cette sensibilisation peut se décliner par le biais de communication régulière et d'une charte informatique remise à chaque nouvel arrivant, qui détaille les usages numériques à respecter et la procédure de déclaration d'un incident. Elle se doit d'être régulièrement rappelée : il peut s'agir, par exemple, de diffusions régulières de messages en interne, lors de réunions ou par le biais d'une newsletter éventuellement étayée par une revue de presse des incidents récents.

La déclaration d'incidents doit être encouragée et, pour ce faire, une réponse non coercitive doit être privilégiée. Il s'agit de responsabiliser les utilisateurs face à des menaces évolutives et non de les sanctionner (sauf en cas d'action délibérée) afin d'éviter une sous-déclaration des incidents.

POUR EN SAVOIR PLUS :

- www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-proteger-vos-donnees-en-sensibilisant-vos-collaborateurs
- cert.ssi.gouv.fr

QUESTION N°11

AVEZ-VOUS FAIT ÉVALUER LA COUVERTURE DE VOTRE POLICE D'ASSURANCE AU RISQUE CYBER ?

PUBLIC : PME
DIFFICULTÉ : MOYENNE

Les sociétés d'assurance proposent de plus en plus des clauses permettant de se prémunir de certains risques d'origine numérique afin d'accompagner les entreprises victimes de cybermalveillance ou de cyberattaques. L'assurance fournit, en cas de sinistre, une assistance juridique ainsi qu'une couverture financière du préjudice (matériel, immatériel, etc.).

Selon les contrats, différents types de protection peuvent être proposés : usurpation d'identité, garanties contre une perte d'exploitation, accompagnement juridique pour une déclaration d'atteinte aux données personnelles, prise en charge d'un accompagnement technique pour la restauration du système d'information après une cyberattaque.

Ces clauses assurantielles peuvent se traduire dans les contrats d'assurance classique ou prendre la forme d'une police d'assurance « cyber » spécifique, bien que ce dernier marché reste encore à être développé, en particulier en matière de jurisprudence concernant l'activation ou non des clauses d'exclusion.

Quelle que soit la forme, il est important de vérifier que les risques les plus redoutés pour la pérennité de l'entreprise soient couverts.

POUR EN SAVOIR PLUS :
www.cybermalveillance.gouv.fr/tous-nos-contenus/france-assureurs

QUESTION N°12

SAVEZ-VOUS COMMENT RÉAGIR EN CAS DE CYBERATTAQUE ?

PUBLIC : PME
DIFFICULTÉ : MOYENNE À EXPERTE

Préparez-vous à l'incident

Les TPE et PME ont tout avantage à identifier préalablement des prestataires spécialisés dans la réponse aux incidents de sécurité.

Pour les TPE et les PME (mais aussi les particuliers et les collectivités), le gouvernement a mis en place la plateforme Cybermalveillance.gouv.fr. Après avoir réalisé un diagnostic en ligne, les victimes accèdent à des conseils personnalisés leur permettant de résoudre leur problème. Elles peuvent également être mises en relation avec des professionnels de proximité pour les assister. N'hésitez pas à vous rapprocher de votre chambre des métiers (CMA) ou de votre chambre du commerce (CCI) : leurs experts peuvent vous orienter vers une assistance appropriée.

Sur le plan technique, **sauvegardez toutes les données de votre entreprise, sans oublier de sauvegarder également les logiciels installés sur votre système d'information (voir la question n°2). Quand un rançongiciel aura chiffré vos données, seule l'existence de sauvegardes intègres vous permettra de redémarrer rapidement votre activité !**

En cas d'incident avéré

Le premier réflexe à avoir en cas d'incident concernant un système d'information est de déconnecter son équipement ou son SI d'entreprise d'Internet. Pour un équipement individuel, cela peut se traduire par la déconnexion de la prise réseau ou la désactivation des services WiFi. Pour un SI d'entreprise, l'action peut être menée sur l'équipement réseau ou le pare-feu d'entreprise. Cela permettra de contenir les actions de l'attaquant et réduira en particulier ses capacités d'exfiltration de données. ▶

Ne pas éteindre ni modifier les ordinateurs et matériels affectés par l'attaque : ils seront utiles aux enquêteurs.

En cas de rançongiciel, ne payez jamais la rançon demandée, des solutions de déchiffrement existent : vous serez assisté par les policiers ou les gendarmes. Vos sauvegardes vous permettront de retrouver une activité normale (voir la question n°2).

Il est recommandé d'ouvrir une main courante pour tracer les actions et les événements liés à l'incident. Chaque entrée de ce document doit contenir, a minima :

- l'heure et la date de l'action ou de l'événement ;
- le nom de la personne à l'origine de cette action ou ayant informé sur l'événement ;
- la description de l'action ou de l'événement.

La tenue d'une main courante régulièrement alimentée tout au long de l'incident va considérablement faciliter l'intervention du prestataire et la résolution du problème.

Pour une PME, il convient de concevoir et de déployer un dispositif de communication (messages, communication interne, communication partenariale, réseaux sociaux, relations presse, etc.). Ce dispositif doit être proposé par le service communication (en lien avec les experts techniques) et porté par les dirigeants de l'entreprise.

La charte informatique peut également informer les collaborateurs de la bonne attitude à avoir en cas d'incident avéré.

Aspects juridiques

Les entreprises traitant des informations personnelles, relevant du Règlement général sur la protection des données personnelles (RGPD) sont soumises au respect des exigences de ce texte. En cas d'incident, elles sont également tenues d'informer la CNIL et leurs clients.

Il est essentiel de porter plainte. Vos matériels affectés et vos journaux seront très utiles aux enquêteurs. En cas de demande de rançon, ne pas la payer.

En cas de fuites de données personnelles, il est obligatoire de faire une déclaration auprès de la CNIL.

POUR EN SAVOIR PLUS :

- www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident
- www.gendarmerie.interieur.gouv.fr/nos-conseils/pour-les-professionnels/cybermenaces-comment-proteger-votre-entreprise
- www.cybermalveillance.gouv.fr/cybermenaces
- www.gouvernement.fr/risques/cybercriminalite
- www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

QUESTION N°13

ENVISAGEZ-VOUS D'UTILISER DES SOLUTIONS *CLOUD* ?

PUBLIC : TOUS
DIFFICULTÉ : FACILE À MOYENNE

« Les offres nuagiques (*cloud*) peuvent-elles m'aider à sécuriser mes données contre les cybercriminels ? ». Au-delà des effets d'annonce et des éléments de langage commerciaux des offreurs *cloud*, une approche méthodique permet d'éviter les écueils d'une solution inadaptée, d'une migration mal évaluée ou de l'usage de services mal maîtrisés (expositions inconsidérées des données, irréversibilité) sous couvert du fait que « ce sera mieux sécurisé dans le *cloud* ».

Identifiez les types de services adaptés

« Une solution *cloud* pour faire quoi ? ». Autrement dit, quel besoin souhaite adresser l'entreprise en voulant utiliser une solution *cloud* ?

L'offre commerciale en matière de *cloud* est assez importante aujourd'hui. On retrouve de nombreux services : messageries, stockage/sauvegarde, comptabilité, ERP, suites bureautiques et collaboratives, etc. En termes techniques, ces offres reposent sur des solutions techniques de type IaaS, PaaS ou SaaS et proposent des niveaux fonctionnels et de sécurité différents. Qui plus est, elles mettent à disposition des clients un grand nombre de services et de fonctions qu'il convient de s'approprier et d'apprendre à bien configurer pour s'assurer du niveau de sécurité, au risque de ne pas être protégé.

La liste des actifs métier (voir la question n°1) et les bonnes pratiques proposées dans ce guide, permettent aux TPE/PME de vérifier l'adéquation des offres de services *cloud* en fonction de leurs besoins fonctionnels et de sécurité. Ce guide peut constituer une sorte de grille de lecture pour les entreprises afin de s'assurer de la présence des fonctionnalités de sécurité utiles pour protéger leurs données en fonction du juste besoin.

« Dois-je privilégier les offres de confiance SecNum*Cloud* ? ». Toutes les offres *cloud* (*cloud* commercial, *cloud* qualifié SecNum*Cloud*, *cloud* privé, etc.) ne répondent pas aux mêmes besoins de sécurité. Les différences en termes de coûts budgétaires sont très variables. Il convient donc de bien analyser les avantages et inconvénients des offres, ne pas hésiter à se faire accompagner par un prestataire spécialisé afin de bien comprendre les conséquences sur le fonctionnement futur de l'entreprise et d'identifier les impacts sur le système d'information.

En ce qui concerne la qualification SecNum*Cloud*, les objectifs de ce « visa de sécurité » ANSSI consistent principalement à garantir un niveau de confiance dans la sécurisation de l'infrastructure ou du service proposé, mais aussi d'apporter une protection juridique contre les lois extracommunautaires. Ces offres peuvent, par exemple, convenir à une entreprise souhaitant protéger ses données contre des risques de contentieux de pays concurrents. Les entreprises sont invitées à mesurer les avantages apportés par ces offres par rapport aux coûts qu'elles peuvent engendrer.

Les offres *cloud*, une opportunité de sécurité mais aussi de nouveaux risques à gérer

Dans la majorité des cas, les offres *cloud* apportent un niveau de service et des fonctions de sécurité qui peuvent rassurer certaines entreprises n'ayant pas de compétence particulière dans le domaine numérique. Toutefois, un certain nombre de points d'attention doivent être pris en compte.

« Dans un contexte d'utilisation d'un service *cloud*, quels sont les risques auxquels je m'expose ? ».

Tout d'abord, et la plupart du temps, les offres *cloud* exposent sur Internet les outils métiers de l'entreprise, ce qui n'était pas forcément le cas avant l'avènement de ce type d'offres. Ensuite, la ou les liaisons via Internet, pour accéder à vos outils métier localisés sur le *cloud*, doivent faire l'objet d'une attention particulière notamment en termes de disponibilité et de confidentialité. Si vous perdez ces liaisons, vous ne pouvez plus travailler avec ces outils. De même, vos communications et vos données transitant sur Internet peuvent être interceptées. Enfin, un défaut de configuration peut exposer les mécanismes d'authentification ou les données de vos services métiers à des tiers.

Vos utilisateurs, vos administrateurs, voire vos prestataires doivent aussi être formés à l'usage de ces outils même si les fournisseurs de services font des efforts pour que l'expérience utilisateur soit la plus simple possible. Il est important que vos collaborateurs adaptent leur pratique lié à l'usage des services dans le *cloud*. Ils doivent donc être sensibilisés aux risques et aux bonnes pratiques à

adopter en termes de sécurité. L'accompagnement aux changements est un axe à ne pas sous-évaluer.

Les technologies *cloud* : ce qu'il vous reste à faire

Les offres *cloud* ne sont pas la réponse ultime à tous les problèmes informatiques. Par ailleurs, les entreprises doivent s'approprier ces technologies et les nombreuses capacités techniques proposées afin de consommer les services *cloud* en ayant conscience des risques résiduels et de les configurer de manière à répondre à leurs besoins de sécurité. Cette démarche vous permettra de faire face à un certain nombre d'écueils dans votre transformation numérique.

En complément des bonnes pratiques évoquées ci-dessus et d'une approche par la gestion des risques propres à l'entreprise, quelques actions plus précises peuvent être mises en œuvre.

POUR LES TPE :

Pour les TPE, il pourra s'agir d'identifier des services *cloud* proposant :

- une authentification à double facteur ;
- des mécanismes de sauvegardes des données en ligne et hors ligne ;
- des alertes en cas d'accès inhabituels ou suspects ;
- un chiffrement des communications (par exemple HTTPS).

Au-delà de s'assurer de l'existence de ces fonctionnalités, il conviendra de les activer et de les configurer judicieusement.

POUR LES PME :

Pour les PME qui disposent de systèmes d'informations existants et internes à l'entreprise, le principal objectif consistera à conserver la cohérence des services numériques et maintenir, voire augmenter, le niveau de sécurité en termes de disponibilité, d'intégrité et de confidentialité.

Un certain nombre d'actions et de vérifications supplémentaires à celles proposées pour les TPE peuvent être adoptées :

- un service d'identification et d'authentification cohérent, voire fédéré avec la base d'authentification de l'entreprise ;
- un contrôle d'accès aux ressources *cloud* strictement réservé aux postes de travail de l'entreprise ; ce contrôle d'accès doit se décliner sous la forme de contrôle des utilisateurs mais aussi des équipements ;

- le cas échéant, des mécanismes de protection des communications sous forme de VPN chiffrés (IPsec ou TLS) ;
- des mécanismes de sauvegardes des données et des services en ligne et hors ligne.

POUR EN SAVOIR PLUS :
www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud

Ce guide présente, en treize questions, des mesures accessibles pour une protection globale de l'entreprise.
Certaines recommandations relèvent des bonnes pratiques, d'autres requièrent un investissement plus important pour lequel votre structure pourra être accompagnée. Elles vous permettront d'accroître votre niveau de sécurisation et de sensibiliser vos équipes aux bons gestes à adopter. À vous de vous en emparer pour protéger votre activité et vos emplois.

En l'absence de préparation, lorsque l'incident survient, il est déjà trop tard. N'attendons pas que le pire arrive. Protégeons-nous !

Version 2.0 – Octobre 2022 – **ANSSI-GP-086**
Dépot légal : octobre 2022

Licence Ouverte/Open Licence (Etalab — V1)
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.ssi.gouv.fr — communication@ssi.gouv.fr